Document 2

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-215379
(43)Date of publication of application : 04.08.2000

(51)Int.Cl. G08C 19/00
G09C 1/00
H04L 9/08
H04N 1/387

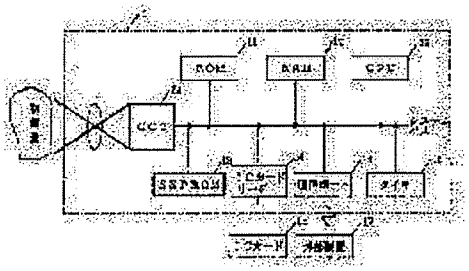
(21)Application number : 11-205709
(22)Date of filing : 21.07.1999

(71)Applicant : RICOH CO LTD
(72)Inventor : KANAI YOICHI
YANAIDA MASUYOSHI

(30)Priority
Priority number : 10326215 Priority date : 17.11.1998 Priority country : JP

## (54) DIGITAL MEASURING EQUIPMENT AND IMAGE MEASURING EQUIPMENT

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain a digital measuring equipment capable of improving the reliability and proving ability in the contents of electronic digital data by providing a key generating means for generating a pair of public key and secret key to be used for the electronic signature of a public key enciphering system from a key generation algorithm.
SOLUTION: This equipment has a RAM 12 to load various algorithms, secret key, sequence number and external certificate key or the like at need and an EEPROM 14 for storing the secret key, public key certificate, sequence number or external certificate key to be used for the electronic signature of the public key enciphering system. A CPU 19 acquires time data from a timer 18, stores them in the RAM 12, simultaneously acquires photographed image data from a CCD 20 and stores them in the RAM 12. Then, the stored image data are compressed. The sequence number is taken out of the EEPROM 13 and at the same time, a sequence number adding '1' to that sequence number is stored in the EEPROM 13.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－215379
（P2000－215379A）
(43)公開日　平成12年８月４日(2000.8.4)

| (51)Int.Cl.' | 識別記号 | ＦＩ | | テーマコード'（参考） |
|---|---|---|---|---|
| Ｇ０８Ｃ　19/00 | | Ｇ０８Ｃ　19/00 | Ａ | |
| Ｇ０９Ｃ　1/00 | ６３０ | Ｇ０９Ｃ　1/00 | ６３０Ｃ | |
| | ６４０ | | ６４０Ｂ | |
| Ｈ０４Ｌ　9/08 | | Ｈ０４Ｎ　1/387 | | |
| Ｈ０４Ｎ　1/387 | | Ｈ０４Ｌ　9/00 | ６０１Ｃ | |

審査請求　未請求　請求項の数13　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願平11－205709

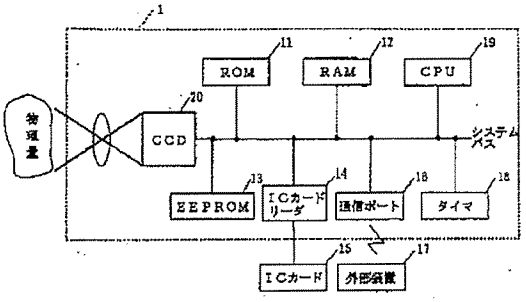
(22)出願日　平成11年７月21日(1999.7.21)

(31)優先権主張番号　特願平10－326215
(32)優先日　平成10年11月17日(1998.11.17)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　谷内田　益義
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100093920
弁理士　小島　俊郎

(54)【発明の名称】　デジタル計測機器及び画像計測機器

(57)【要約】
【課題】　本発明は、電子デジタルデータの内容の信頼性及び証明力を高められるデジタル計測機器及び画像計測機器を提供することを目的とする。
【解決手段】　物理的な計測対象を計測し、計測した物理量の計測データに対して公開鍵暗号方式の電子署名を付与して計測データを管理する、本発明に係るデジタル計測機器は、公開鍵暗号方式の電子署名に用いる、少なくとも一対の公開鍵と秘密鍵を鍵生成アルゴリズムによって生成する鍵生成手段を有する。



【特許請求の範囲】

【請求項１】　物理的な計測対象を計測し、計測した物理量の計測データに対して公開鍵暗号方式の電子署名を付与して計測データを管理するデジタル計測機器において、

公開鍵暗号方式の電子署名に用いる、少なくとも一対の公開鍵と秘密鍵を鍵生成アルゴリズムによって生成する鍵生成手段を有することを特徴とするデジタル計測機器。

【請求項２】　前記計測データに対して前記秘密鍵を用いて計算した電子署名を前記計測データと共に記録する請求項１記載のデジタル計測機器。

【請求項３】　前記秘密鍵により署名された、外部から書き替え不可能な公開鍵証明書を記憶する請求項１記載のデジタル計測機器。

【請求項４】　計測された順番を示す、外部からの書き替え不可能なシーケンス番号を収容し、該シーケンス番号を前記計測データと共に記録する請求項１記載のデジタル計測機器。

【請求項５】　少なくとも１つの外部認証コードを収容し、該外部認証コードに対する外部認証が成立したときに前記鍵生成アルゴリズム、前記電子署名及び前記シーケンス番号の更新を可能とする請求項１～４のいずれかに記載のデジタル計測機器。

【請求項６】　画像データに対して公開鍵暗号方式の電子署名を付与する画像計測機器において、

画像の特徴量を画像データフォーマットの画像付帯情報の一部として有し、画像計測機器の秘密鍵を用いて画像付帯情報から電子署名を計算し、計算した電子署名を画像付帯情報として画像データフォーマット中に格納することを特徴とする画像計測機器。

【請求項７】　電子署名を計算する際に画像付帯情報のいずれかの情報を使用したのかを画像付帯情報として画像データフォーマット中に格納しておく請求項６記載の画像計測機器。

【請求項８】　画像の特徴量を含む画像付帯情報について特徴量を計算し、計算した特徴量を画像付帯情報として格納すると共に、特徴量を元に画像計測機器の秘密鍵を用いて電子署名を計算し、計算した電子署名を画像付帯情報として画像データフォーマット中に格納する請求項６記載の画像計測機器。

【請求項９】　画像の特徴量を含む画像付帯情報について特徴量を計算し、計算した特徴量を画像付帯情報として格納すると共に、特徴量を元に画像計測機器の秘密鍵を用いて電子署名を計算し、計算した電子署名を画像付帯情報として画像データフォーマット中に格納し、また特徴量を元に画像計測機器に装着された外部記憶手段に格納された秘密鍵を用いて電子署名を計算し、当該電子署名も画像付帯情報として画像データフォーマット中に格納する請求項６記載の画像計測機器。

【請求項１０】　電子署名の計算に使用する特徴量を計算する際に使用する画像付帯情報は、画像データのシリアル番号を含む請求項６～９のいずれかに記載の画像計測機器。

【請求項１１】　電子署名の計算に使用する特徴量を計算する際に使用する画像付帯情報は、画像計測機器のシリアル番号を含む請求項６～９のいずれかに記載の画像計測機器。

【請求項１２】　電子署名の計算に使用する特徴量を計算する際に使用する画像付帯情報は、電子署名の計算に使用する秘密鍵の対となる公開鍵を含む請求項６～９のいずれかに記載の画像計測機器。

【請求項１３】　電子署名の計算に使用する特徴量を計算する際に使用する画像付帯情報は、電子署名の計算に使用する秘密鍵の対となる公開鍵を公開鍵証明書の形で含む請求項６～９のいずれかに記載の画像計測機器。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデジタル計測機器及び画像計測機器に関し、詳細にはデジタルカメラ、スキャナ、センサ、ＦＡＸ（モデム）などから得られた入力をデジタルデータに変換し、そのデジタルデータに対して管理や伝送等の処理を施す装置のデータセキュリティに関する。

【０００２】

【従来の技術】近年、情報の電子化が急速に進み、あらゆる情報が電子データとしてネットワークやポータブルメディアを介して相互にやり取りされるようになっており、その電子データのセキュリティを確保するために様々な技術が開発されている。一般に検討されている電子データのセキュリティ技術は、主にデータの秘匿技術やデータの改ざん検知技術、データへのアクセス権の管理（認証を含む）技術等、データの内容には着目せず、端なる塊として扱うセキュリティ技術が多い一方、その電子データの内容が元々正しいかどうかに関する技術開発はあまりなされていなかった。しかし、セキュリティを確保しようとしている元々のデータが不正なものであれば、そのデータのセキュリティを確保しても何の意味もなさない。元々のデータが最初から人為的な操作によって電子的に生成されたものであれば、そのデータの内容が正しいことを保証するには、従来の技術のように、そのデータを作成した作成者もしくはそのデータに関して責任をもっている者の電子署名を付加するなどの処理を施すことになる。

【０００３】そこで、従来例として、米国特許第５，４９９，２９４号明細書には、デジタルカメラにそのデジタルカメラ固有のプライベートキーを格納し、そのデジタルカメラで撮影された画像ファイルに対して当該プライベートキーを用いて電子署名を計算して画像ファイルとともに媒体に記録するという方法が開示されている。

詳細には、デジタルカメラに格納しているプライベートキーはデジタルカメラ内のＳｅｃｕｒｅ　ＰｒｏｃｅｓｓｏｒにＲＯＭ化して記録されており外部から読み出すことができないようになっている。また、そのプライベートキーに対応するパブリックキーをデジタルカメラの本体に刻印する。更に、デジタルカメラで撮影した画像の周辺部にそのパブリックキーや撮影状況を示すパラメータなどを印字し、その画像全体に対して電子署名を施すようにしている。そのため、そのデジタルカメラで撮影した画像は証明力が高められている。なお、デジタルカメラに対応するパブリックキーはデジタルカメラの製造メーカが広く公開することを前提としている。

【０００４】

【発明が解決しようとする課題】しかしながら、上記従来例によれば、撮影した画像ファイルと、それに対してデジタルカメラが計算した電子署名ファイルが別々であるために画像ファイルをパソコン等に移した際にそれらの関連付けがわからなくなる可能性がある。そのため、せっかく画像ファイルの証明力を高める処理を施したのにもかかわらず、電子署名ファイルがどれだかわからなくなり結局画像ファイルの真正性を検証することができなくなるという問題があった。

【０００５】また、プライベートキーとパブリックキーのペアをデジタルカメラの製造メーカが生成し、カメラの内部に記録するようにしているが、デジタルカメラ製造メーカがプライベートキーを知っていることは証明力を低下させることに繋がるという問題もあった。

【０００６】更に、デジタルカメラ内蔵のタイマの設定を製造時点において設定した後、変更できないようにしているが、タイマが徐々に狂ってしまうことは当然起こりうることであり、正しい時刻に設定し直せないのは問題であった。それに、タイマの電源であるリチウムイオン電池が切れてしまうと時刻そのものの記録ができなくなるのも問題であった。

【０００７】また、上記従来例ではデジタルカメラ個々に割り振ったパブリックキー全てを製造メータが広く公開することになっているが、デジタルカメラが非常に数多く製造される場合を考えると、その数の分だけパブリックキーを公開するというのは煩雑さが増して画像の真正性検証の際に膨大なパブリックキーリストの中から該当するパブリックキーを探し出さなければならないという問題があった。

【０００８】更に、デジタルカメラのような一般ユーザ向けのデジタル機器を想定しているために、誰がそのデータを記録したのか、などについて全く考慮されていないという問題があった。例えば、ＣＴ装置やデジタル内視鏡装置などの医療用計測装置の場合には特に誰がそのデータを計測（撮影）したのかが重要となることがあるからである。

【０００９】また、デジタルカメラのような一般ユーザ向けの比較的安価なライフサイクルの短いデジタル機器を想定しているため、装置内部の電子署名アルゴリズムの追加・入れ替えや鍵の更新に関しては考慮されておらず、新しい製品モデルにおいて新しいアルゴリズムを搭載するとしか述べられていない。しかし、例えばＣＴ装置のような高額なデジタル医療機器の場合には、そのライフサイクルも長く、装置の寿命より短い機関で暗号アルゴリズムの強度が相対的に弱くなってしまうという可能性があるという問題があった。

【００１０】本発明はこれらの問題点を解決するためのものであり、電子デジタルデータの内容の信頼性及び証明力を高められるデジタル計測機器及び画像計測機器を提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明は前記問題点を解決するために、物理的な計測対象を計測した物理量の計測データを管理するデジタル計測機器において、公開鍵暗号方式の電子署名に用いる少なくとも一対の公開鍵と秘密鍵を鍵生成アルゴリズムによって生成する鍵生成手段を有することに特徴がある。よって、生成した秘密鍵は製造メーカすら知り得ない。

【００１２】また、計測データに対して秘密鍵を用いて計算した電子署名を計測データと共に記録することや秘密鍵により署名された外部から書き替え不可能な公開鍵証明書を記憶することにより、秘密鍵を公開せずとも公開鍵証明書を作成する際に使用した秘密鍵に対応する公開鍵のみで良い。

【００１３】更に、計測された順番を示す、外部からの書き替え不可能なシーケンス番号を収容し、該シーケンス番号を計測データと共に記録することにより、計測データの前後関係が混乱しないようにすることができる。

【００１４】また、少なくとも１つの外部認証コードを収容し、該外部認証コードに対する外部認証が成立したときに鍵生成アルゴリズム、電子署名及びシーケンス番号の更新を可能とすることにより、計測したデータの証明力を長期間維持できる。

【００１５】更に、別の発明として、画像の特徴量を画像データフォーマットの付帯情報の一部として有し、画像付帯情報から画像計測機器の秘密鍵を用いて電子署名を計算し、画像付帯情報として画像データフォーマット中に追加格納することにより、画像計測機器より得られた画像に電子署名を埋め込むので画像計測機器で撮影した画像が改ざんされていないかどうか検証できるようになっているし、画像の特徴量を画像付帯情報として格納し、電子署名を計算する際にどの画像付帯情報を使用して署名を計算したのかを明確できる。そうすることで電子署名を格納したことによって画像データの、証拠写真と関わらない部分の付帯情報についても変更や追加ができるようになった。

【００１６】

【発明の実施の形態】公開鍵暗号方式の電子署名に用いる少なくとも一対の公開鍵と秘密鍵を鍵生成アルゴリズムによって生成する鍵生成手段を有する。

【００１７】

【実施例】以下、本発明の実施例を図面に基づいて説明する。はじめに、電子データの内容、特に物理量の計測データとは、具体例を挙げれば、デジタルカメラで撮影した画像データや医療で使用するＣＴ（Ｃｏｍｐｕｔｅｄ　Ｔｏｍｏｇｒａｐｈｙ）装置で計測、計算した再構成画像データなどが挙げられる。これらのデータのように、計測したデータからその計測装置特有の処理（デジタルカメラの場合には画像の圧縮処理や階調変換処理などＣＴ装置の場合にはＦＢＰ（Ｆｉｌｔｅｒｅｄ　Ｂａｃｋ　Ｐｒｏｊｅｃｔｉｏｎ）法　よる画像再構成処理など）を施した後のデータなど、計測した物理量と関連付けを保証する必要が生じる（そのデータを他人に渡ったり、見せたりする場合には保証する必要が生じるものと考えられる）電子データが対象となる。そして、デジタルカメラやＣＴ装置など、一般には計測装置と呼ばれないような装置であっても、以上のような背景から「デジタル計測機器」と呼ばれている。

【００１８】図１は本発明の第１の実施例に係るデジタル計測機器の構成を示すブロックである。なお、本実施例のデジタル計測機器としてデジタルカメラを例として以下説明するものとする。同図に示す本実施例は、電子署名用の暗号アルゴリズム（例えばＲＳＡとＭＤ５など）、及び外部認証に使用する暗号アルゴリズム（例えばＤＥＳ（Ｄａｔｅ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）。このＤＥＳは秘密鍵暗号方式の暗号アルゴリズムであるが外部認証に使用できればどのような方式の暗号アルゴリズムでも構わない）、画像データ圧縮アルゴリズム（例えばＪＰＲＧ）、乱数発生アルゴリズム、メイン制御プログラムを格納するＲＯＭ１１と、メイン制御プログラム、各種アルゴリズム、秘密鍵、シーケンス番号、外部認証鍵等が必要に応じてロードされるＲＡＭ１２と、公開鍵暗号方式の電子署名に使用する秘密鍵、公開鍵証明書（公証機関の署名と公開鍵）、シーケンス番号や外部認証鍵を格納するＥＥＰＲＯＭ１３と、撮影したデジタル撮影画像データにシーケンス番号、時刻、電子署名などを付加したデジタル画像情報を記録する、例えばメモリカード等のＩＣカード１５の当該情報を読み出し／書き込みを行うＩＣカードリーダ１４、外部装置１７との通信によるやり取りを行うための通信ポート１６と、時刻データを取得するタイマ１８と、各種の演算を行いかつ各構成要素を制御するＣＰＵ１９と、撮影した画像を電子データに変換するＣＣＤ２０とを含んで構成されている。

【００１９】次に、本実施例の動作について説明すると、シャッタボタンが押されると、ＣＰＵ１９はタイマ１８から時刻データを取得し、それをＲＡＭ１２に記憶すると同時にＣＣＤ２０から撮影画像データを取得してＲＡＭ１２に格納する。そして、格納された画像データを圧縮する。また、ＥＥＰＲＯＭ１３からシーケンス番号を取り出すと同時にシーケンス番号に１加えたシーケンス番号をＥＥＰＲＯＭ１３に格納する。圧縮された画像データの先頭に先に取り出したシーケンス番号と、タイマ１８から取得した時刻データを付加する。そして、できあがった画像情報に対してその電子署名を先の画像情報に付加して、一つの塊としての撮影情報としてＩＣカード１５に格納する。秘密鍵、公開鍵証明書、シーケンス番号、時刻設定を変更する際に、予め行うべき外部認証処理は、外部認証に使用するアルゴリズムに例えばＤＥＳを使用する場合を例に取ると以下の手順で行う。

【００２０】先ず、内部で乱数を発生させ、その乱数を外部装置に送出する。外部装置から認証コードを受け取り、先に生成した乱数を外部認証鍵により暗号化したコードと比較する。それらのコードが一致すれば外部認証が成立したこととし、セキュリティステータス（これはＲＡＭで管理しているフラグ。初期状態はＦＡＬＳＥとする）をＴＲＵＥに変更する。外部から秘密鍵、公開鍵証明書、シーケンス番号、時刻設定の変更を要求された場合には、先ず内部で管理しているセキュリティステータスを参照し、それがＦＡＬＳＥとなっている場合には要求を受け付けない。一方ＴＵＲＥとなっている場合には要求を受け付け、その要求に応じた処理を行う。処理を行うとセキュリティステータスをＦＡＬＳＥに変更する。

【００２１】次に、本実施例における計測データに対する処理の流れについて以下に説明する。先ず、既に装置のキーペア（このキーペアはプライベートキーとパブリックキーのペアのことである）が生成されているかどうかを調べ（ステップＳ１０１）、されていない場合は処理を終了するが、生成されていれば図１のＩＣカード１５からユーザ公開鍵証明書を取得する（ステップＳ１０２）。ＣＣＤ２０から計測データ（撮影データ）を取得し、更にタイマ１８から現在時刻を取得する（ステップＳ１０３，Ｓ１０４）。そして、取得した計測データに必要な処理、例えば圧縮、ＣＴ画像再構成、標準データフォーマットへの変換などを施し、処理済みの計測データを取得する（ステップＳ１０５）。次に、ＥＥＰＲＯＭ１３からプライベートキー・公開鍵証明書・シーケンス番号を取得する（ステップＳ１０６）。取得したシーケンス番号に１増加させてＥＥＰＲＯＭ１３に格納する（ステップＳ１０７）。処理済みの計測データに現在時刻及びシーケンス番号を追加されてたものを計測情報とする（ステップＳ１０８）。この計測情報に対してハッシュ値を計算する（ステップＳ１０９）。計算したハッシュ値はプライベートキーにより暗号化され、装置の電子署名を計算する（ステップＳ１１０）。上記計算されたハッシュ値をＩＣカードに渡し、ユーザのプライベー

トキーにより暗号化したユーザ電子署名を取得する（ステップＳ１１１）。そして、計測情報に装置の電子署名及び公開鍵証明書を追加し、装置の署名済みの計測情報とする（ステップＳ１１２）。更に、ユーザ電子署名やユーザ公開鍵証明書を追加して装置・ユーザの署名済み計測情報とする（ステップＳ１１３）。出来上がった署名済み計測情報をファイルとして大容量外部記録媒体に記録する（又は通信ポート１６から外部装置に送出する）（ステップＳ１１４）。

【００２２】このように、暗号処理機能及び記憶機能を持つＩＣカード等の外部記憶手段を使用してユーザの署名を生成し、ユーザの公開鍵証明書と共に装置の署名済計測情報に付与しているだけで計測装置自身はユーザの認証を行っていない。これは署名済み計測情報を検証すればユーザが誰であったか「後で」認証するができるためである。一方、計測装置自身が予めユーザを認証できれば他の方法であっても構わなく、計測装置にとってユーザが認証されてさえいれば単にユーザ名をシーケンス番号などと共に処理済み計測データに付与して電子署名処理を施しても構わない。ＩＣカードを使用しない場合には計測装置がＩＣカードリーダ１４を搭載する必要はない。装置の公開鍵証明書には装置のシリアル番号、製造メータ名などが記載されており、ユーザの公開鍵証明書にはユーザを特定できるユーザ名や所属などが記載されていることを想定している。装置の公開鍵証明書については外部からの要求に応じて装置が外部に送出することを可能とする。また、本実施例では、計測情報を作成してからすぐに電子署名の作成を行っているが電子署名の作成には計算時間がかかるため、連続して計測を行いたい場合には不都合が生じる可能性がある。そこで、作成した計測情報はそのまま大容量外部記憶媒体に記録しておき、後で外部に送出する前、又は大容量記憶媒体を計測情報から取り外す前に電子署名を作成・付与するようにしても良い。その場合には、電子署名を付与するまでは大容量外部記憶媒体が計測装置本体から取り外せないようにするなど電子署名を付与していない計測情報に外部装置からアクセスできないようにする必要がある。

【００２３】また、単に付帯情報（現在時刻、シーケンス番号、公開鍵証明書など）を処理済み計測データの後ろに追加するようにしているが、例えばＪＰＥＧ画像の場合には画像データフォーマットとして任意のデータを埋め込むことができるため、それを利用してその部分にそれら付帯情報を記録することもできる。そうすることで、電子署名が埋め込まれたファイルでありながら、既存の画像表示プログラムなどが処理することも可能となる。その際注意しなければならないのは、ＴＩＦＦなどの場合には画像データがどこからはじまっているのか、その絶対位置をタグとして持っているため、電子署名を埋め込んだ場合にはその絶対位置がずれてしまうことになる。そこで、そのような問題を回避するために、図３に示すように、予め電子署名を埋め込む分だけ領域を確保し、その領域は予め決められた値で埋めておき、その上でデータ全体に対してハッシュ値を計算し、電子署名を生成する。そして、生成された電子署名を予め確保しておいた領域に埋め込むということも可能である。データ計測を行う前に予めキーペア生成処理を実行していなければならない。この処理は例えば計測装置製造メーカが工場において出荷前に実行する。

【００２４】次に、キーペア生成処理について図４及び図５に基づいて説明すると、既にキーペアが計測機器のＥＥＰＲＯＭに記録されているかどうかを調べ（ステップＳ２０１）、キーペアが記録されていれば生成する必要がないので処理を終了する。一方、キーペアが記録されていないならば、図４に示すように、鍵生成アルゴリズムによりキーペアを生成する（ステップＳ２０２）。そして、生成したキーペアはＥＥＰＲＯＭに記録される（ステップＳ２０３）。次に、キーペアのうちパブリックキーは通信ポートを介して外部装置に送信される（ステップＳ２０４）。図４に示すように、外部装置においてパブリックキーに対して公開鍵証明書を作成され、当該公開鍵証明書は通信ポートを介してデジタル計測機器に渡される（ステップＳ２０５，Ｓ２０６）。そして、公開鍵証明書はＥＥＰＲＯＭに記録される（ステップＳ２０７）。

【００２５】また、計測装置の内部タイマを設定する処理は簡単な例で言えば計測装置にキーパッドを取付け、キーパッドからパスワードを入力し、計測装置が内部に保持しているパスワードと照合して正しければタイマの設定変更を許可するといった方法が考えられる。他にも上記本実施例のように計測装置がＩＣカードリーダを搭載しているので、特定のＩＣカードが挿入去れている場合にのみタイマの設定を変更できるようにすることも考えられる。挿入されているのが特定のＩＣカードかどうかを検証するためには例えば以下のような方法をとることができる。図６に示すように予め計測機器メーカのパブリックキーを計測装置内部に格納しておく。そして、計測装置が最初に生成した乱数と、ＩＣカードからの認証コードを復号した乱数’が一致すればＩＣカードは秘密の鍵を持っていることになり、特定のコードであることが認証できる。

【００２６】暗号アルゴリズムの更新処理については、例えばタイマの設定処理で説明すると、特定のＩＣカードを挿入している最中にのみ通信ポートを介して新しい暗号処理プログラムを受け取ることができるようにするようなことが考えられる。又は図７に示すように、暗号処理プログラムに製造メーカの電子署名を付与して計測装置に渡すと、計測装置がその電子署名を検証し、正しい電子署名であることが検証できれば、その暗号処理プログラムを内部記憶媒体に格納して暗号処理に使用する方法も考えられる。この例においても計測装置には予め

製造メーカの公開鍵を保持していることを想定している。暗号処理プログラムには、ハッシュ値を計算するアルゴリズムやキーペアを生成するアルゴリズム、そして暗号化するアルゴリズムや復号するアルゴリズムが含まれていることを想定している。

【００２７】また上記では暗号アルゴリズムの更新処理として述べたが、暗号アルゴリズムについては更新するのではなく、単に追加しかできないようにしても良い。後から登録する暗号アルゴリズムは当然のことながら強度が高いものを使用するべきであるが、古い暗号処理プログラムを持ってきて誰かが不正に計測装置にインストールした場合に、既に最新の暗号処理プログラムを搭載している計測装置の証明力が低下することを防ぐことができる。それだけでなく、古いアルゴリズムに比べ、最新の暗号アルゴリズムには欠陥が見つかる可能性が大きい。そのため、計測情報には古いアルゴリズムの電子署名と、新たにインストールした暗号アルゴリズムによる電子署名を両方付与するようにしても良い。また、暗号アルゴリズムについては、新しいアルゴリズムはより計算量を必要とする可能性が大きいため、暗号処理プログラムとしての入れ替えでなく、暗号処理プログラムを実行するプロセッサの入れ替えを行うようにしても良い。その場合、暗号処理プロセッサが正当な製造メーカにより作られたものかどうか認証する必要があるが、その仕組みは先に特定のＩＣカードかどうかを検証する処理と全く同じ処理を適用することができる。暗号処理プロセッサモジュールは例えばＰＣＭＣＩＡカードなどのような形態が考えられる。又は、暗号処理プロセッサと計測装置との間の物理的なインタフェースを特殊なものにしたり、計測装置のプロセッサと暗号処理プロセッサとの間のプロトコルを特殊なものにして非公開にするなどの方法を取っても良い。そのような場合には暗号処理プロセッサを認証する必要はない。計測装置のプロセッサと暗号処理のためのプロセッサに分けた場合の計測装置の構成は図８のようになるが詳細な説明は省略する。

【００２８】上記第１の実施例では、計測データの中に電子署名を格納するフィールドを予約し、その部分を予めＮＵＬＬパディングした状態の計測データ全体に対してデジタル計測機器が電子署名を計算し、その電子署名を先の予約フィールドに格納する方法をとっていた。この方法の場合、計測データに電子署名を格納した後で、さらに計測データの中に他の情報、例えばコメントなどを格納したくなった場合に問題があった。つまり、後から他の属性情報を計測データに付け加えたり、計測データの証明力に関わらない属性情報であってもそれに変更を加えたりすると、計測データ自身が異なるデータとなってしまい、電子署名の検証が不可能になる可能性があった。

【００２９】そこで、以下に説明する第２の実施例は、電子署名を計算した対象を明確にすることで、後から別の属性情報を追加した際にも電子署名の検証を可能にするものである。

【００３０】第２の実施例についてＥｘｉｆ（Ｅｘｃｈａｎｇｅａｂｌｅ ｉｍａｇｅ ｆｉｌｅ ｆｏｒｍａｔ ｆｏｒ ｄｉｇｉｔａｌ ｓｔｉｌｌ ｃａｍｅｒａ）の画像フォーマットを例にして説明する。図９はＥｘｉｆの画像フォーマットの内容を示す図である。なお、電子署名と、その電子署名の属性情報は、画像撮影条件に関する情報を記述するＥｘｉｆ ＩＦＤ及びＧＰＳ情報を記述するＧＰＳＩＦＤ、と並列にセキュリティ情報を記述するためのタグの集まりであるＳｅｃｕｒｉｔｙ ＩＦＤというものを独自に定義し、格納することを実施例として考えている。その際に、Ｅｘｉｆ ＩＦＤやＧＰＳ ＩＦＤには計測データ（デジタルカメラの場合にはデジタル写真データ）の証明力を高めるのに役に立つ情報、例えば日付や撮影場所など、計測条件に関わる情報が含まれているため、この情報は改ざんされないよう電子署名により保護したい情報であり、また当然のことながら、計測データ本体そのものと、それを再生するのに必要となる情報についても保護したい対象である。具体的にはＤＱＴマーカからＥＯＩマーカの手前までも保護したいのである。したがって、例えばＥｘｉｆ ＩＦＤとＧＰＳＩＦＤとＤＱＴマーカからＥＯＩマーカまでについての電子署名であるということを電子署名の属性情報として管理すれば良いことになるが、規格上はＥｘｉｆＩＦＤやＧＰＳ ＩＦＤの中にはコメントを記録できるようになっており、後からＥｘｉｆ ＩＦＤの中にコメントを追加してしまった場合、Ｅｘｉｆ ＩＦＤが以前と異なる状態になってしまうため、電子署名の検証ができなくなってしまう。そこで、電子署名を計算する際に使用したデータを特定する情報を電子署名の属性情報として記録するようにする。

【００３１】次に、撮影されたデジタル画像に対して電子署名を付与する処理手順を図１０に基づいて以下に説明する。ここでは、すでにデジタル画像はＪＰＥＧ（Ｅｘｉｆ）フォーマットに変換されていることを想定している。

【００３２】（１）先ず、保護したい（証拠にしたい）画像データストリーム（例えばＤＱＴマーカからＥＯＩマーカの手前まで）に対して、ＳＨＡ－１やＭＤ５といったハッシュアルゴリズムでハッシュ値（特徴量）を計算する（ステップＳ１００１）。この計算された値をイメージハッシュ値と呼ぶ。

【００３３】（２）イメージハッシュであることを示すタグ番号を用い、Ｖａｌｕｅ部として先のイメージハッシュ値を持つＴＬＶデータエレメント（Ｔａｇ（図中「Ｔ」で表記），Ｌｅｎｇｔｈ（図中「Ｌ」で表記），Ｖａｌｕｅ（図中「Ｖ」で表記））を作成する（ステップＳ１００２）。この作成されたものをイメージハッシュデータエレメントと呼ぶ。

【００３４】（３）Ｅｘｉｆフォーマットに対して新しく独自に定義したＳｅｃｕｒｉｔｙＩＦＤに、先のイメージハッシュデータエレメントを追加する（ステップＳ１００３）。

【００３５】（４）Ｅｘｉｆ　ＩＦＤ、ＧＰＳ　ＩＦＤ、Ｓｅｃｕｒｉｔｙ　ＩＦＤに含まれる、証拠写真として役に立つデータエレメントのタグのリストを作成する（ステップＳ１００４）。これをハッシュタグリストと呼ぶ。なお、このハッシュタグリストにはＥｘｉｆ　ＩＦＤの中の撮影日時データエレメントや、Ｓｅｃｕｒｉｔｙ　ＩＦＤの中のイメージハッシュデータエレメント、撮影者データエレメントなども含まれることになる。

【００３６】（５）ハッシュタグリストに含められたタグに対応する各データエレメントのＶａｌｕｅ部（Ｖａｌｕｅ部が４バイトを超えていて別の場所に本来のＶａｌｕｅ部が記録されている場合には、その別の場所に格納されているＶａｌｕｅ部）を順にＳＨＡ－１やＭＤ５といったハッシュアルゴリズムにかけ、一つのハッシュ値を計算する（ステップＳ１００５）。この計算された値をデータハッシュ値と呼ぶ。

【００３７】（６）データハッシュであることを示すタグ番号を用い、Ｖａｌｕｅ部としてそのデータハッシュ値を持つＴＬＶデータエレメントを作成する（ステップＳ１００６）。この作成されたものをデータハッシュデータエレメントと呼ぶ。

【００３８】（７）先のデータハッシュ値を、デジタルカメラの内部記憶媒体にあるプライベートキーで暗号化する（ステップＳ１００７）。この暗号化されたものをデータ署名と呼ぶ。

【００３９】（８）データ署名であることを示すタグ番号を用い、Ｖａｌｕｅ部としてそのデータ署名の値を持つＴＬＶデータエレメントを作成する（ステップＳ１００８）。この作成されたものをデータ署名データエレメントと呼ぶ。

【００４０】（９）Ｓｅｃｕｒｉｔｙ　ＩＦＤに先のデータハッシュデータエレメントと、データ署名データエレメントを追加する（ステップＳ１００９）。

【００４１】（１０）できあがったＥｘｉｆ画像データをデジタルカメラの大容量記憶媒体に記録する。

【００４２】詳細には述べていないが、ＴＩＦＦのデータ記述方法と同様、ＴＬＶのＶの部分が４バイトを超える場合（ハッシュ値などは８バイト程度）には、Ｖに別の場所を指すオフセットポインタを記録し、その別の場所にＶの値を記録するようにする。

【００４３】このようにして作成された電子署名付きのデジタルカメラの画像は、以下のような処理手順によって、その真正性が検証できる。

【００４４】先ず、ＪＰＥＧ（Ｅｘｉｆ）画像から、データ署名データエレメントのＶａｌｕｅ部を取り出す。データ署名をデジタルカメラのパブリックキーで復号する。ＪＰＥＧ（Ｅｘｉｆ）画像から、データハッシュデータエレメントのＶａｌｕｅ部を取り出す。検証用データハッシュ値とデータハッシュ値が一致するかどうか確認する。一致しなければ、画像データに何かしらの改ざんが行われている。ＪＰＥＧ（Ｅｘｉｆ）画像から、ハッシュタグリストデータエレメントのＶａｌｕｅ部を取り出す。ハッシュタグリストに記録されているタグに該当するデータエレメントのＶａｌｕｅ部を順に取り出し、ハッシュアルゴリズムにかけてハッシュ値を計算する。再計算ハッシュ値と先のハッシュ値が一致するかどうか確認する。一致しなければ、画像データに何かしらの改ざんが行われている。ＪＰＥＧ（Ｅｘｉｆ）画像から、イメージハッシュデータエレメントのＶａｌｕｅ部を取り出す。ＪＰＥＧ（Ｅｘｉｆ）画像から、保護している画像データストリーム部を取り出し、ハッシュアルゴリズム（ＳＨＡ－１やＭＤ５など）にかけてハッシュ値を計算する。検証用イメージハッシュ値とイメージハッシュ値が一致するかどうか確認する。一致しなければ、画像データに何かしらの改ざんが行われている。以上の処理で異常が見つからなければ、画像データは改ざんされていない（改ざんされた可能性は極めて低い）ため、真正性が確保されていると判断できる。

【００４５】このような処理は、電子署名を埋め込む際の処理手順を逆に辿ったようなやり方をしているが、当然のことながら、電子署名を埋め込むのと同じ手順を追ってハッシュ値などを計算し、最後にプライベートキーで暗号化する部分を、逆に画像データに埋め込まれているデータ署名をパブリックキーで復号してデータハッシュ値を比較するという方法をとることもできる。

【００４６】なお、上記実施例ではデジタルカメラを例として説明したがスキャナ等の画像読取手段によって光学的に読み取った画像データあるいはＦＡＸ等で送受信された画像データ等のように画像処理装置によって得られた画像データにも適用できることは言うまでもない。更に、本発明は上記実施例に限定されるものではなく、特許請求の範囲内の記載であれば多種の変形や置換可能であることは言うまでもない。

【００４７】

【発明の効果】以上説明したように、本発明によれば、物理的な計測対象を計測した物理量の計測データを管理するデジタル計測機器において、公開鍵暗号方式の電子署名に用いる少なくとも一対の公開鍵と秘密鍵を鍵生成アルゴリズムによって生成する鍵生成手段を有することに特徴がある。よって、生成した秘密鍵は製造メーカすら知り得ない。

【００４８】また、計測データに対して秘密鍵を用いて計算した電子署名を計測データと共に記録することや秘密鍵により署名された外部から書き替え不可能な公開鍵証明書を記憶することにより、秘密鍵を公開せずとも公

開鍵証明書を作成する際に使用した秘密鍵に対応する公開鍵のみで良い。

【００４９】更に、計測された順番を示す、外部からの書き替え不可能なシーケンス番号を収容し、該シーケンス番号を計測データと共に記録することにより、計測データの前後関係が混乱しないようにすることができる。

【００５０】また、少なくとも１つの外部認証コードを収容し、該外部認証コードに対する外部認証が成立したときに鍵生成アルゴリズム、電子署名及びシーケンス番号の更新を可能とすることにより、計測したデータの証明力を長期間維持できる。

【００５１】更に、画像計測機器により得られた画像に電子署名を埋め込むので画像計測機器で得た画像が改ざんされていないかどうか検証できるようになっている。その際、デジタル画像に電子署名を格納するとデジタル画像そのものが電子署名を格納したことによって変化してしまうことがある。また、後から画像付帯情報を追加することもできなくなる。それを防ぐために、画像のイメージデータストリーム部の特徴量を画像付帯情報として格納し、電子署名を計算する際には、どの画像付帯情報を使用して署名を計算したのかを明確にした。そうすることで電子署名を格納したことによって画像データの、証拠写真と関わらない部分の付帯情報についても変更や追加ができるようになった。

【図面の簡単な説明】

【図１】本発明の第１の実施例に係るデジタル計測機器の構成の概略を示すブロック図である。

【図２】本実施例における計測データに対する処理の流れを示すフローチャートである。

【図３】本実施例における電子署名の格納の様子を示す図である。

【図４】本実施例におけるキーペア生成処理の様子を示す図である。

【図５】本実施例におけるキーペアの生成処理の流れを示すフローチャートである。

【図６】本実施例における外部認証の様子を示す図である。

【図７】本実施例における暗号アルゴリズムの更新処理の様子を示す図である。

【図８】入れ替え可能な暗号処理プロセッサを付加した例の構成を示すブロック図である。

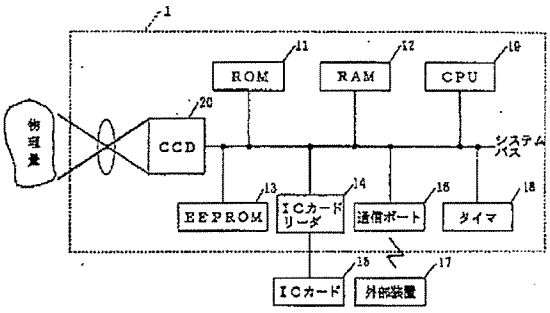
【図９】画像フォーマットの内容を示す図である。

【図１０】本発明の第２の実施例に係る画像計測機器における電子署名の格納処理手順の様子を示す図である。

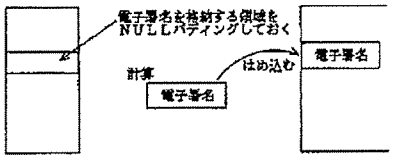
【符号の説明】

１１：ＲＯＭ、１２：ＲＡＭ、１３：ＥＥＰＲＯＭ、１４：ＩＣカードリーダ、　１５：ＩＣカード、１６：通信ポート、１７：外部装置、１８：タイマ、１９：ＣＰＵ、２０：ＣＣＤ、２１：暗号処理プロセッサ。

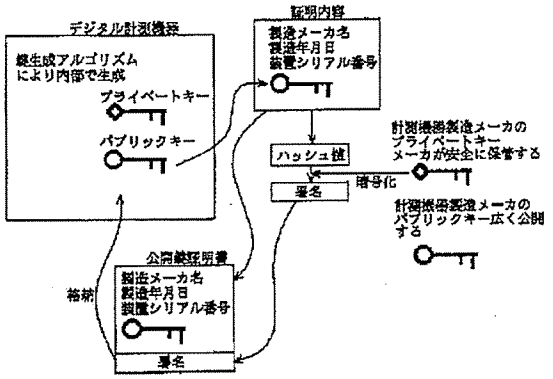
【図１】



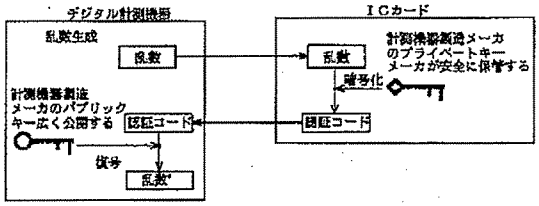

【図３】



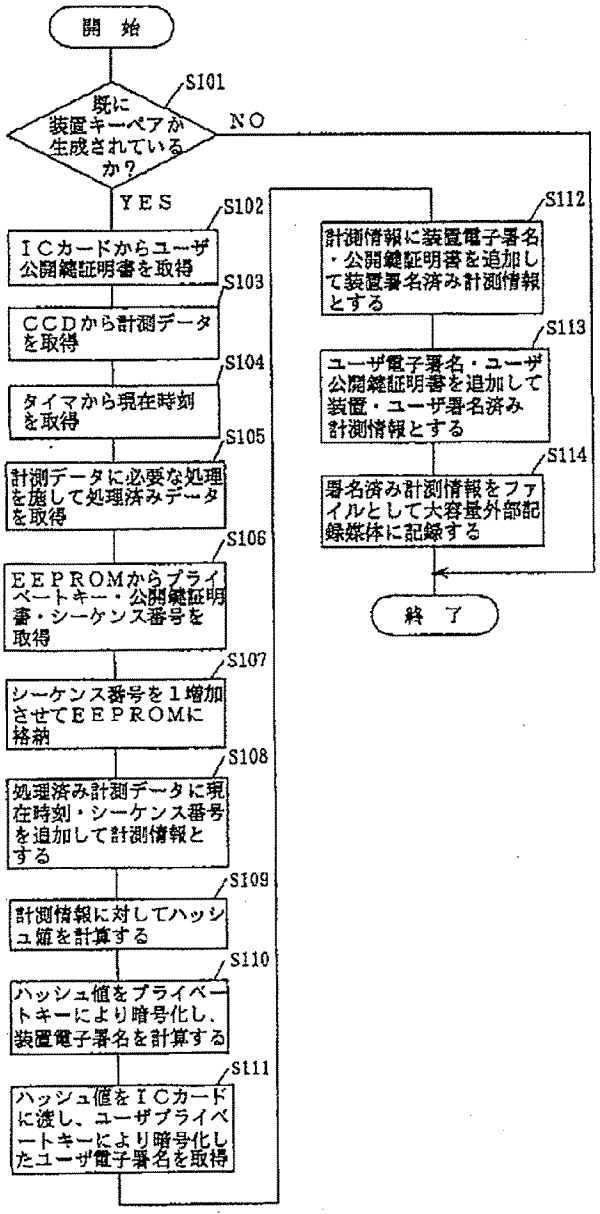

【図４】



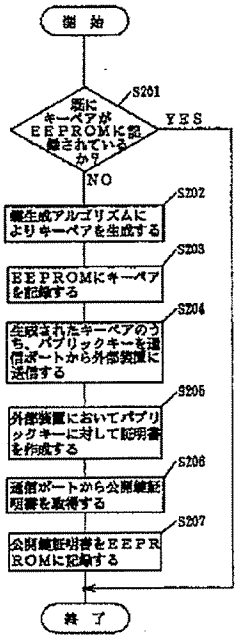

【図６】



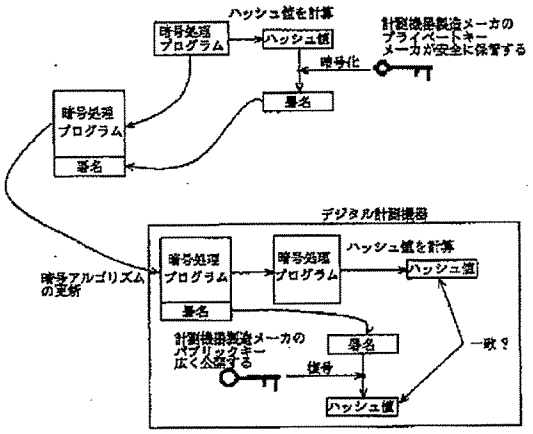
【図２】


開　始
S101
既に装置キーペアが生成されているか？
NO
YES
S102
ＩＣカードからユーザ公開鍵証明書を取得
S103
ＣＣＤから計測データを取得
S104
タイマから現在時刻を取得
S105
計測データに必要な処理を施して処理済みデータを取得
S106
ＥＥＰＲＯＭからプライベートキー・公開鍵証明書・シーケンス番号を取得
S107
シーケンス番号を１増加させてＥＥＰＲＯＭに格納
S108
処理済み計測データに現在時刻・シーケンス番号を追加して計測情報とする
S109
計測情報に対してハッシュ値を計算する
S110
ハッシュ値をプライベートキーにより暗号化し、装置電子署名を計算する
S111
ハッシュ値をＩＣカードに渡し、ユーザプライベートキーにより暗号化したユーザ電子署名を取得
S112
計測情報に装置電子署名・公開鍵証明書を追加して装置署名済み計測情報とする
S113
ユーザ電子署名・ユーザ公開鍵証明書を追加して装置・ユーザ署名済み計測情報とする
S114
署名済み計測情報をファイルとして大容量外部記録媒体に記録する
終　了

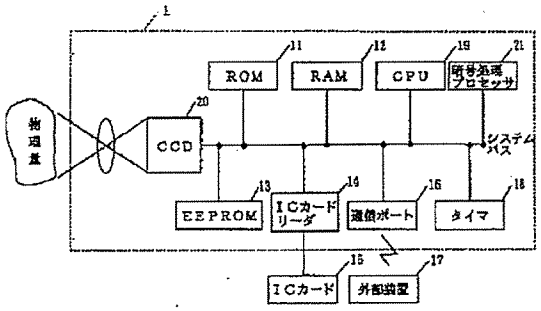
【図５】


開　始
S201
既にキーペアがＥＥＰＲＯＭに記録されているか？
YES
NO
S202
鍵生成アルゴリズムによりキーペアを生成する
S203
ＥＥＰＲＯＭにキーペアを記録する
S204
生成されたキーペアのうち、パブリックキーを通信ポートから外部装置に送信する
S205
外部装置においてパブリックキーに対して証明書を作成する
S206
通信ポートから公開鍵証明書を取得する
S207
公開鍵証明書をＥＥＰＲＯＭに記録する
終　了

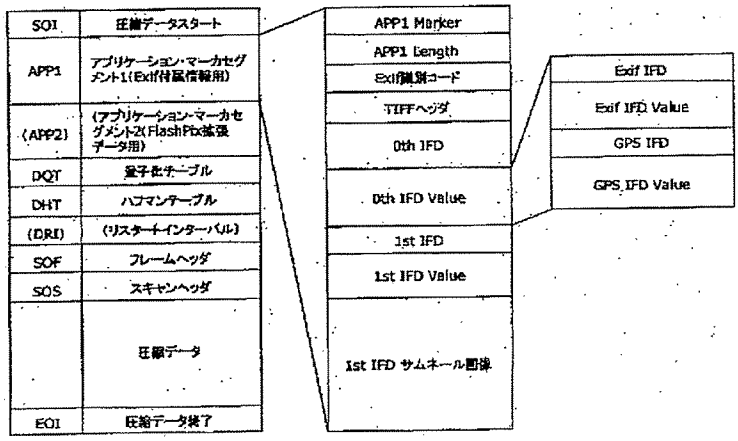
【図７】


ハッシュ値を計算
暗号処理プログラム
ハッシュ値
暗号化
計測機器製造メーカのプライベートキー メーカが安全に保管する
署名
暗号処理プログラム
署名
デジタル計測機器
暗号処理プログラム
暗号処理プログラム
ハッシュ値を計算
ハッシュ値
暗号アルゴリズムの更新
署名
計測機器製造メーカのパブリックキー広く公表する
復号
一致？
ハッシュ値

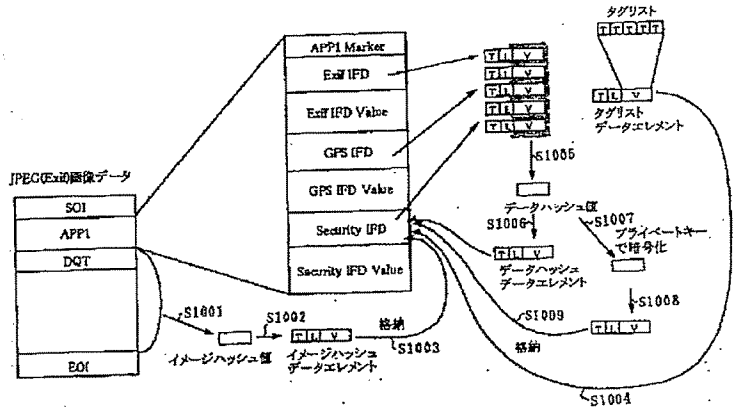
【図８】


1
ROM
RAM
CPU
暗号処理プロセッサ
11
12
19
21
物理量
CCD
20
システムバス
EEPROM
ICカードリーダ
通信ポート
タイマ
13
14
16
18
ICカード
外部装置
15
17

【図９】


SOI
圧縮データスタート
APP1
アプリケーション・マーカセグメント1(Exif付属情報用)
(APP2)
(アプリケーション・マーカセグメント2(FlashPix拡張データ用))
DQT
量子化テーブル
DHT
ハフマンテーブル
(DRI)
(リスタートインターバル)
SOF
フレームヘッダ
SOS
スキャンヘッダ
圧縮データ
EOI
圧縮データ終了
APP1 Marker
APP1 Length
Exif識別コード
TIFFヘッダ
0th IFD
0th IFD Value
1st IFD
1st IFD Value
1st IFD サムネール画像
Exif IFD
Exif IFD Value
GPS IFD
GPS IFD Value

【図１０】


JPEG(Exif)画像データ
SOI
APP1
DQT
EOI
APP1 Marker
Exif IFD
Exif IFD Value
GPS IFD
GPS IFD Value
Security IFD
Security IFD Value
タグリスト
タグリストデータエレメント
S1005
データハッシュ値
S1006
S1007
プライベートキーで暗号化
データハッシュデータエレメント
S1008
S1009
格納
S1004
S1001
イメージハッシュ値
S1002
イメージハッシュデータエレメント
格納
S1003

フロントページの続き

| (51) Int. Cl.[7] | 識別記号 | FI | | テーマコード(参考) |
|---|---|---|---|---|
| | | H04L 9/00 | 601F | |